

#2

501.37212X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. KAYASHIMA, et al
Serial No.:
Filed: May 19, 1999
Title: NETWORK MANAGEMENT SYSTEM
Group:

jc542 U.S. PRO
09/314629
05/19/99

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

May 19, 1999


Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 10-136614 filed May 19, 1998.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, PERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/nac
Attachment
(703) 312-6600

219701001 US1

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JCS42 U.S. PRO
09/314629
05/19/99

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

1998年 5月19日

出願番号
Application Number:

平成10年特許願第136614号

出願人
Applicant (s):

株式会社日立製作所

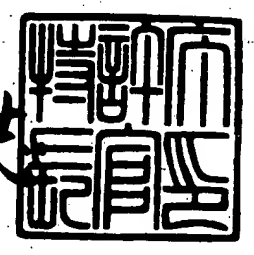
CERTIFIED COPY OF
PRIORITY DOCUMENT

Best Available Copy

1999年 4月 9日

特許庁長官
Commissioner,
Patent Office

佐山建志



【書類名】 特許願

【整理番号】 PNT970452

【提出日】 平成10年 5月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00
H04L 9/14
H04L 9/16
H04L 9/30
H04L 9/32
G06F 17/60

【発明の名称】 ファイアウォール統括管理システム

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

【氏名】 藤山 達也

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

【氏名】 萱島 信

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

【氏名】 寺田 真敏

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5 0 3 0 番地 株式会社日立製作所ソフトウェア開発本部内

【氏名】 荻野 孝明

【特許出願人】

【識別番号】 000005108
 【氏名又は名称】 株式会社日立製作所
 【代表者】 金井 務

【代理人】

【識別番号】 100061893
 【弁理士】
 【氏名又は名称】 高橋 明夫
 【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100086656
 【弁理士】
 【氏名又は名称】 田中 恭助
 【電話番号】 03-3661-0071

【手数料の表示】

【予納台帳番号】 011626
 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ファイアウォール統括管理システム

【特許請求の範囲】

【請求項1】 ネットワークの管理単位間にファイアウォールを設けたネットワークに適用するファイアウォール統括管理システムにおいて、

ファイアウォールに管理情報の設定をおこなうための管理サーバを設け、その管理サーバのマネージャプログラムから、設定情報を送信することによって、

ネットワーク形態から見て、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなえることを特徴とするファイアウォール統括管理システム。

【請求項2】 各々のファイアウォールは、

中継プログラムと、

中継経路情報を格納する中継経路テーブルとを有し、

前記マネージャプログラムから、通信要求があったときには、

前記中継プログラムは、前記中継テーブルを参照し、適切な中継先のファイアウォールに通信要求を出し、

次の経路となるファイアウォールに接続を順次中継して、

最終的に、前記マネージャプログラムが、設定対象となるファイアウォールに対して設定情報を送信できるようにすることを特徴とする請求項1記載のファイアウォール統括管理システム。

【請求項3】 前記接続を中継するファイアウォールの中継プログラムが、前記管理サーバに対する認証をおこなうことを特徴とする請求項2記載のファイアウォール統括管理システム。

【請求項4】 前記管理サーバ上の前記マネージャプログラムが、前記接続を中継するファイアウォールに対する認証をおこなうことを特徴とする請求項2記載のファイアウォール統括管理システム。

【請求項5】 前記管理サーバ上の前記マネージャプログラムと、前記中継サーバの前記中継プログラムの通信を暗号化することを特徴とする請求項2ない

し請求項4記載のいずれかのファイアウォール統括管理システム。

【請求項6】 各々のファイアウォールに、エージェントプログラムを設け

そのファイアウォールに管理情報の設定をおこなうときには、

前記エージェントプログラムは、前記管理サーバ上のマネージャプログラムのエージェントとして、管理情報の設定を自らにおこなうことを特徴とする請求項1ないし請求項5記載のファイアウォール統括管理システム。

【請求項7】 前記ファイアウォールにあるエージェントプログラムは、前記管理サーバのマネージャプログラムから、設定情報を送信されたときに、前記管理サーバに対する認証をおこなうことを特徴とする請求項6記載のファイアウォール統括管理システム。

【請求項8】 前記管理サーバのマネージャプログラムは、サービスを受けるクライアントのクライアントアドレスと、サービスを提供するサーバのサーバアドレスとから、設定情報を送信するファイアウォールを特定することを特徴とする請求項1ないし請求項7記載のいずれかのファイアウォール統括管理システム。

【請求項9】 前記管理サーバのマネージャプログラムは、管理者から入力された情報にしたがって、設定情報を生成し、各々のファイアウォールに設定情報を送信することを特徴とする請求項1ないし請求項8記載のいずれかのファイアウォール統括管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ファイアウォール統括管理システムに係り、大規模なネットワークでセキュリティのために複数のファイアウォールが必要なイントラネットなどに好適なシステムであって、それら複数のファイアウォールに対して、一括して管理のための情報を設定することを可能にすることにより、管理者の労力の軽減に資するファイアウォール統括管理システムに関する。

【0002】

【従来の技術】

インターネットのようなオープンなネットワーク上で、あたかも専用線のような使い勝手を実現するVPN (Virtual Private Network) が注目を集めつつある。このVPN技術では、私的なネットワークをオープンなネットワーク上に接続するため、不正侵入を阻止するためのセキュリティ対策として、ファイアウォール (Firewall) を用いるのが一般的になっている。このファイアウォールでは、特定のユーザのみにアクセスを許可するアクセス制御や、データの暗号化によりシステムとしての安全度を高めている。

【0003】

普通、ファイアウォールは、各ネットワークの管理単位 (インターネットでは、「ドメイン」) 間に設けられるので、複数のネットワークの管理単位を接続するときは、システム全体として複数のファイアウォールが存在することになる。そして、これらのファイアウォールの設定は、それぞれ独立に行うわけではなく、相互に関連を持つため、全体を統括して管理する必要がある。

【0004】

このようなVPNに関係する全てのファイアウォールの設定を、統括的に管理する製品として、CheckPoint社の「FireWall-1」がある。FireWall-1は、「管理モジュール」と「ファイアウォールモジュール」により構成されており、個々のファイアウォールに対する設定を、一つの管理モジュールからおこなうことができる。セキュリティに関する定義情報であるセキュリティポリシーを生成すると、管理モジュールは、対象となるファイアウォールモジュールに対して設定データを送付する。

【0005】

【発明が解決しようとする課題】

FireWall-1に代表される従来技術は、管理モジュールが複数のファイアウォールモジュールを管理することにより、各ファイアウォールが保護するネットワークや利用ユーザの設定を管理モジュールから一括しておこなうことができる。

【0006】

しかしながら、上記従来技術では、実際にファイアウォールに対して、管理情報を設定しなければならない管理者の労力軽減ということについては、限定的なものに止まっていた。というのも、特に認証されたユーザのみ複数のファイアウォールを越える通信を実行できるように設定するには、管理者は、以下のように二段階からなる煩わしい作業をおこなう必要があったからである。

【0007】

- ・通信経路上にあるファイアウォールを特定する。

【0008】

- ・特定した各ファイアウォールにユーザ登録と動作設定とをおこなう。

【0009】

また、上記従来技術は、ファイアウォールモジュールにより保護された内部ネットワーク上に設置された内部ファイアウォールモジュールに設定情報を送信するなどの管理作業をするには、管理モジュールが直接内部ファイアウォールモジュールへ通信可能であることを必要とする。

【0010】

しかしながら、以下の状況のような場合には、ファイアウォールモジュールとの通信が不可能になる。

【0011】

- ・中継の経路上にあるファイアウォールモジュールが、管理用通信プロトコルをフィルタリングして通さないとき
- ・内部ネットワークがローカルアドレスを使用するとき

このような場合には、ローカルなネットワークの内部の端末から管理情報を設定しなければならなかったり、管理通信プロトコルをフィルタリングしないように設定するなど、いずれも管理者にとっては煩雑な作業が必要であった。

【0012】

本発明は、上記従来技術の問題点を解決するためになされたもので、イントラネット、VPNのような複数のファイアウォールを有するネットワークシステムにおいて、それらのファイアウォールを統括的に管理して、ファイアウォールに

対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するファイアウォール統括管理システムを提供することを目的とする。

【0013】

【課題を解決するための手段】

上記目的を達成するために、本発明のファイアウォール統括管理システムに係る発明の構成は、ネットワークの管理単位間にファイアウォールを設けたネットワークに適用するファイアウォール統括管理システムにおいて、ファイアウォールに管理情報の設定をおこなうための管理サーバを設け、その管理サーバのマネージャプログラムから、設定情報を送信することによって、ネットワーク形態から見て、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなえるようにしたものである。

【0014】

より詳しくは、上記ファイアウォール統括管理システムにおいて、各々のファイアウォールは、中継プログラムと、中継経路情報を格納する中継経路テーブルとを有し、前記マネージャプログラムから、通信要求があったときには、前記中継プログラムは、前記中継テーブルを参照し、適切な中継先のファイアウォールに通信要求を出し、次の経路となるファイアウォールに接続を順次中継して、最終的に、前記マネージャプログラムが、設定対象となるファイアウォールに対して設定情報を送信できるようにするようにしたものである。

【0015】

また詳しくは、上記ファイアウォール統括管理システムにおいて、前記接続を中継するファイアウォールの中継プログラムが、前記管理サーバに対する認証をおこなうようにしたものである。

【0016】

別に詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバ上の前記マネージャプログラムが、前記接続を中継するファイアウォールに対する認証をおこなうようにしたものである。

【0017】

さらに詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバ上の前記マネージャプログラムと、前記中継サーバの前記中継プログラムの通信を暗号化するようにしたものである。

【0018】

さらにまた詳しくは、上記ファイアウォール統括管理システムにおいて、各々のファイアウォールに、エージェントプログラムを設け、そのファイアウォールに管理情報の設定をおこなうときには、前記エージェントプログラムは、前記管理サーバ上のマネージャプログラムのエージェントとして、管理情報の設定を自らにおこなうようにしたものである。

【0019】

また詳しくは、上記ファイアウォール統括管理システムにおいて、前記ファイアウォールにあるエージェントプログラムは、前記管理サーバのマネージャプログラムから、設定情報を送信されたときに、前記管理サーバに対する認証をおこなうようにしたものである。

【0020】

さらに詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバのマネージャプログラムは、サービスを受けるクライアントのクライアントアドレスと、サービスを提供するサーバのサーバアドレスとから、設定情報を送信するファイアウォールを特定するようにしたものである。

【0021】

さらにまた詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバのマネージャプログラムは、管理者から入力された情報にしたがって、設定情報を生成し、各々のファイアウォールに設定情報を送信するようにしたものである。

【0022】

【発明の実施の形態】

以下、本発明に係る一実施形態を、図1ないし図23を用いて説明する。

【0023】

〔ファイアウォール統括管理システムのネットワーク構成〕

先ず、図1を用いて本実施形態に係るファイアウォール統括管理システムのネットワーク構成について説明する。

図1は、本実施形態に係るファイアウォール統括管理システムのネットワーク構成図である。

【0024】

本実施形態では、プロトコルとしてインターネットのデファクトスタンダードになっているTCP (Transmission Control Protocol) / IP (Internet Protocol) を用いるものとして説明する。

【0025】

ドメイン12a～12eは、ネットワークが管理される単位であり、一つのドメインは、同じ方針で管理されている。また、各ドメインは、不特定多数のユーザがアクセス可能なオープンなネットワークであるインターネット11で結ばれている。さらに、各ドメインと外部のネットワークとの間には、外部からの不正侵入を防ぐためのアクセス制御をおこなう装置であるファイアウォール14a～14dが設けられている。

【0026】

ドメイン2には、管理サーバ13と管理端末15が接続されている。管理サーバ13は、ファイアウォールを管理する機能を提供するサーバである。管理端末15は、管理者がファイアウォールの管理作業をおこなうために設けられた端末である。従来では、ファイアウォールの管理は、ファイアウォールと同じドメインに接続されている端末からおこなっていたが、本発明では、これらの管理サーバ13と管理端末15により、他のドメインに接続されているファイアウォールの管理情報も設定できるところに特徴がある。

【0027】

なお、本実施形態では、管理作業用のユーザインタフェースを提供する管理端末15を用意したが、ネットワークの構成上、管理サーバから管理作業をおこなうようにしても良い。

【0028】

各ドメイン12a～12dは、オープンなインターネットを利用して、仮想的にプライベートなネットワークとして利用する、いわゆるVPN (Virtual Private Network) を実現しているものとする。その際に、セキュリティのためには、ファイアウォールは必須の設備であるといえることができる。

【0029】

〔ファイアウォール統括管理システムの各ハードウェア構成〕

次に、図2ないし図4を用いて本実施形態に係るファイアウォール統括管理システムを構成している各々のハードウェア構成について説明する。

まず、図2を用いて本実施形態の管理サーバのハードウェア構成について説明する。

図2は、本実施形態に係る管理サーバ13のハードウェア構成図である。

【0030】

管理サーバ13は、プロセッサ21と、固定ディスク22と、メモリ27と、入出力制御部211と、ネットワーク制御部213とで構成される。

【0031】

プロセッサ21は、計算機内のハードウェア間の制御とプログラムの処理をおこなうユニットである。固定ディスク22は、大容量の補助記憶装置であり、プログラムやテーブルを格納する装置である。メモリ27は、プログラムをロードしたり、一時的なデータを格納する装置であり、通常は半導体素子で構成される。入出力制御部211は、外部に記憶された入出力装置、例えば、ディスプレイやキーボード212などを制御する。ネットワーク制御部213は、他の計算機との間の回線を制御する部分である。

【0032】

固定ディスク22には、本発明のファイアウォール統括管理システムを実現するためのプログラムと各種のテーブルが格納される。マネージャプログラム23は、管理サーバ上で動作する管理プログラムであり、管理者から入力された情報に基づき、ファイアウォールに設定するための制御情報を生成し、ファイアウォールに送信する機能を持つ。認証・暗号通信モジュール22aは、マネージャプ

プログラム 23 から呼び出され、認証、暗号通信をおこなう機能を受け持つ。ファイアウォール構成情報テーブル 24 は、ファイアウォールとドメインとの接続関係を記載したテーブルである。ユーザ情報テーブル 25 は、様々なユーザ情報を格納するテーブルであり、ユーザ毎のネットワーク利用形態情報と利用経路情報とから成っている。中継経路テーブル 26 は、送信先アドレスと次の接続先アドレスである中継先アドレスとを記載したテーブルであり、設定情報をファイアウォールに送信するときに、接続を中継するファイアウォールのアドレスを格納する。

【0033】

なお、ここに出てきたテーブルの内容と機能については後に詳細に説明する。

【0034】

一方、メモリ 27 は、上記のようにプログラムを固定ディスクからロードしてきて格納したり、一時的なデータを保持するための装置であり、論理的に各エリアに分割して用いられる。マネージャプログラムエリア 28 は、マネージャプログラム 22 を格納するエリア、認証・暗号通信モジュールエリア 29 は、認証・暗号通信モジュールがロードされるエリア、ファイアウォール設定情報テーブルエリア 215 は、ファイアウォールの管理情報設定のときに、ダイナミックに生成されるファイアウォール設定情報テーブル 215 を格納するエリアであり、経由ファイアウォールテーブルエリア 214 は、経由ファイアウォールテーブルを格納するエリア、中継経路テーブルエリア 210 は、中継経路テーブルエリアを格納するエリアである。ファイアウォール設定情報テーブル 215 と経由ファイアウォールテーブルエリア 214 についても後述する。

【0035】

次に、図 3 を用いて本実施形態のファイアウォールのハードウェア構成について説明する。

図 3 は、本実施形態に係るファイアウォール 14a～14d のハードウェア構成図である。

【0036】

ファイアウォール 14a～14d は、プロセッサ 31 と、固定ディスク 32 と

、メモリ36と、ネットワーク制御部313とで構成される。各々の機能は、管理サーバ13のときと同様である。

【0037】

ファイアウォール14a～14dの固定ディスク32にも、管理サーバ13のときと同様に、本発明のファイアウォール統括管理システムを実現するためのプログラムと各種のテーブルが格納される。エージェントプログラム33は、ファイアウォール上でマネージャプログラムのエージェント（代理人）として働くプログラムであり、マネージャプログラムから送信されてくるファイアウォールの設定情報を受信し、それをファイアウォールが持っている各テーブルに設定する。中継経路テーブル35は、管理サーバ13のときと同様に、送信先アドレスと次の接続先アドレスである中継先アドレスとを記載したテーブルであり、設定情報をファイアウォールに送信するときに、接続を中継するファイアウォールのアドレスを格納する。中継プログラム34は、ファイアウォールの設定情報を持つパケットを設定対象となるファイアウォールに送信するときに、その経路にあたるファイアウォールが、接続を中継するプログラムであり、前記中継経路テーブル35に基づいて接続を次のファイアウォールに中継する機能を持つ。認証・暗号通信モジュール33aは、エージェントプログラム33から呼び出され、認証、暗号通信をおこなう機能を受け持つ。ユーザ登録テーブル312は、ユーザ登録情報を格納し、ユーザがサービスを受けるときに認証をおこなうためのテーブルである。アクセス制御テーブル313は、ユーザがサービスを受けるときに必要な各種情報を格納するテーブルである。経路制御テーブル314は、ユーザがサービスを受けるときのパケットの経路情報を格納するテーブルである。

【0038】

また、ファイアウォール14a～14dのメモリ36には、エージェントプログラムエリア37と、中継プログラムエリア38と、中継経路テーブルエリア39と、認証・暗号通信モジュールエリア310に分割されてデータが格納される。エージェントプログラムエリア37は、エージェントプログラム33を格納するエリア、中継プログラムエリア38は、中継プログラム34が格納されるエリア、中継経路テーブルエリア39は、中継経路テーブルを格納するエリア、認証

・暗号通信モジュールエリア 310 は、認証・暗号通信モジュールがロードされるエリアである。

【0039】

次に、図 4 を用いて本実施形態の管理端末のハードウェア構成について説明する。

図 4 は、本実施形態に係る管理端末 15 のハードウェア構成図である。

【0040】

管理端末 15 は、プロセッサ 41 と、固定ディスク 42 と、メモリ 45 と、入出力制御部 46 と、ネットワーク制御部 48 とで構成される。管理端末 15 も、各々の機能は、管理サーバ 13 のときと同様である。

【0041】

管理端末 15 上の固定ディスク 42 には、ユーザインターフェイスプログラム 43 が、格納されていて、実行されるときには、メモリ上のユーザインターフェイスプログラムにロードされる。ユーザインターフェイスプログラムは、ネットワークの管理者にファイアウォールの制御操作のためのユーザインターフェイスを提供するプログラムである。

【0042】

〔ファイアウォール統括管理システムのファイアウォール設定処理〕

次に、図 5 ないし図 19 を用いて本発明に係るファイアウォール統括管理システムにおいて、ファイアウォールの設定をする処理について説明する。

図 5 は、本発明に係るファイアウォール統括管理システムが、ファイアウォールの設定をする処理を模式的に示した図である。

【0043】

この図 5 で示された例では、図 1 に示したシステム構成のもとで、特に認証されたユーザ 197 のみがクライアントからサーバ 199 にアクセスできるようにファイアウォールに設定する場合を想定している。

【0044】

管理サーバ 13 が、このようなファイアウォールの設定処理をおこなうときには、以下の処理を順におこなうことになる。これを、図 5 をふまえて項を分けて

説明しよう。

【0045】

- (1) 設定対象ファイアウォールを特定する処理 191
- (2) ファイアウォール毎に設定情報を生成する処理 192
- (3) ファイアウォール毎の設定情報を各ファイアウォールに送信する処理 193
- (4) 各ファイアウォールが設定情報を受信し、それを設定する処理 194
- (5) ファイアウォールが接続を中継する処理 195

(1) 設定対象ファイアウォールを特定する処理 191

先ず、図6ないし図10を用いて設定対象ファイアウォールを特定する処理 191について説明する。

図6は、管理者が、設定情報を入力するときの管理端末15上の入力画面51を示す図である。

図7は、管理サーバ13上のファイアウォール構成情報テーブル24を示す図である。

図8は、マネージャプログラム22が設定するファイアウォールを特定する処理を示すフローチャートである。

図9は、経由ドメインリスト214の内容を状態毎に示した図である。

図10は、管理サーバ13上の経由ファイアウォールテーブル214を示す図である。

【0046】

ファイアウォールとして、ネットワークの防衛のために有効に機能するためには、そのネットワークの形態から見て設定が必要なファイアウォールを特定し、そのファイアウォールに対して、サービスを受ける利用者の利用形態を想定した設定をする必要がある。そのために、先ず管理者は、図5に示される管理端末15から、必要な設定情報を入力する。

【0047】

ユーザ識別子（グローバルユーザ名）52は、サービスを受けるネットワーク全域において、一意的でグローバルに通用する名称である。クライアントアドレ

ス53は、ユーザが利用するクライアントのアドレスであり、サーバアドレス54は、ユーザがサービスを受けるサーバのアドレスである。このアドレスは、計算機またはネットワークを一意的に識別するアドレスであり、表記の仕方については、DNS (Domain Name System) に基づくドメイン形式で記述し、ネットワーク全体で通用するアドレスにしておく必要がある。

【0048】

サービス名55には、ユーザが利用するサービス名を入力する。この図5に示される例は、グローバルユーザ名が「abc」であるユーザが、「ドメイン1」から「ドメイン3」に「telnet」でアクセスするサービスを前提として、ファイアウォールの設定をおこなう場合である。

【0049】

管理端末15からの入力が終わると、管理端末15上のユーザインタフェースプログラム43は、入力画面51に入力された情報を、管理サーバ13に送信する。そして、管理サーバ13上のマネージャプログラム23は、送信されてくる入力情報を取得する。

【0050】

設定するファイアウォールを特定するためには、管理サーバ15のマネージャプログラム23がネットワークの形態を押さえる必要がある。そのために、ドメインとファイアウォールの接続関係を記述したものが図7に示されるファイアウォール構成情報テーブル24である。

【0051】

ファイアウォール構成情報テーブル24は、図7に示されるように、ドメインを示すドメイン名フィールド61と、そのドメインに接続されているファイアウォールを示すファイアウォール名フィールド62と、ドメイン名フィールド61に記述したドメインとファイアウォールを隔てて隣接するドメインを示す隣接ドメイン名フィールド63から構成されている。

【0052】

本実施形態で採り上げる図1に示すネットワーク環境の場合、ドメイン2 (12b) には、ファイアウォール1 (14a) とファイアウォール2 (14b) が

接続されている。そして、ファイアウォール1 (14 a) 側には、ドメイン1 (12 a) が隣接しており、ファイアウォール2 (14 b) 側には、インターネット (11) が隣接している。このときには、ファイアウォール構成情報テーブル24の各フィールドには、エントリ64 a, 64 b, 64 c, 64 fに示す内容が登録される。

【0053】

次に、図8および図9を用いてマネージャプログラム23が、設定対象ファイアウォールを特定する処理手順を説明する。

【0054】

この処理は、マネージャプログラム23が、ユーザの利用するクライアントアドレス53、サーバアドレス54、およびファイアウォール構成情報テーブル24とを用いて、経由するファイアウォールを特定することにより、設定対象となるファイアウォールを決定するものである。

【0055】

ドメイン形式のアドレスは、ホスト名とクライアントの属するドメイン名が合成された形式をとる。したがって、図7 (a) に示されるように、マネージャプログラム23は、まず、ドメイン形式で与えられたクライアントアドレス53から、ホスト名を除くことによりクライアントの属するドメイン名 (クライアントドメイン名) を取得する。例えば、ドメイン形式が、「www.xyz.co.jp」であるときには、wwwがホスト名であり、クライアントドメイン名は、xyz.co.jpとなる。そして、経由ドメインリスト214の先頭に得られたクライアントドメイン名を追加する (S71)。

【0056】

経由ドメインリスト214は、クライアントからサーバまでの間に経由するドメイン名を保存するリストである。経由ドメインリスト214が具体的にどのような様子に用いられるかについては、後に図9を用いて詳細に説明する。

【0057】

次に、クライアントドメイン名に対して、処理A (S74) を実行する (S72)。処理Aは、再帰的呼出し手続きであり、経由ドメインリストを取得する処

理である。したがって、この処理を抜け出てきたときには、クライアントからサーバまでの経由ドメインリストが完成されている。

【0058】

最後に、経由ドメインリスト中の連続するドメイン名とファイアウォール構成情報テーブルとから、その間のファイアウォール名を取得することにより、経由するファイアウォールのリスト（経由ファイアウォールリスト）を取得する（S73）。この経由ファイアウォールリストは、図10に示される経由ファイアウォールテーブル214のエントリとして格納される。

【0059】

経由ファイアウォールテーブル214は、設定対象ファイアウォールを特定する処理の結果を格納するためのテーブルであり、クライアントアドレスフィールド81とサーバアドレスフィールド82と経由ファイアウォールリストフィールド83とから構成される。クライアントアドレスフィールド81とサーバアドレスフィールド82は、それぞれクライアントのアドレスとサーバのアドレスを格納するフィールドである。経由ファイアウォールリストフィールド83は、前述の如く、設定対象ファイアウォールを特定する処理の結果として、クライアントアドレス53からサーバアドレス54までの経路上にあるファイアウォールのリストを格納したものがある。すなわち、この経由ファイアウォールリストフィールド83に記載された一連のファイアウォールが、クライアントがサーバからサービスにあたって、マネージャプログラム23が、設定対象とするファイアウォールである。

【0060】

次に、上記の処理A（S74）について説明する。

【0061】

この処理Aに与えられる引数は、ドメイン名、ファイアウォール構成情報テーブル24、経由ドメインリスト241である。また、この処理Aは、再帰的呼出し手続き（Recursive Call）であることに注意する。

【0062】

まず、マネージャプログラム53は、与えられたドメイン名とファイアウォー

ル構成情報テーブル24のドメイン名フィールド61とが一致するエントリを検索する。そして、一致したエントリの隣接ドメイン名フィールド63に記載されたドメイン名からリストを作成する(S75)。これを、隣接ドメイン名リストとすることにする。

【0063】

この隣接ドメイン名リストに要素がない場合(S76)、処理Aから抜ける。

【0064】

隣接ドメイン名リストに要素がある場合(S76)、そのリストからドメイン名を1つ選択する。選択したドメイン名が、経由ドメイン名リストで既に使用されているならば、隣接ドメイン名リストから別のドメイン名を選択する(S77)。経由ドメイン名リストで使用されていないならば、経由ドメイン名リストに追加する(S78)。

【0065】

そして、今追加したドメイン名がサーバが属するドメイン名(サーバドメイン名)に等しいか否かを調べる(S79)。追加したドメイン名がサーバが属するドメイン名(サーバドメイン名)に等しいならば(S79)、経由ドメイン名リストを別領域に保存する(S710)。

【0066】

この時点で保存されたドメイン名リストが、この処理の答えとなる経由ドメイン名リストになる。

【0067】

そして、経由ドメイン名リストの一番最後に追加されたドメイン名を削除する。これは、手続きが再帰的呼出しを使っているため、経由ドメイン名の探索を元に戻して処理するために必要な手続きである。

【0068】

そして、隣接ドメイン名リストを調べる処理に戻る(S76)。

【0069】

追加したドメイン名がサーバドメイン名に等しくないならば(S79)、追加したドメイン名を引数にして、再帰的に、処理Aを呼び出す(S712)。

【0070】

処理Aから抜け出たときには、経由ドメインリストの一番最後に追加されたドメイン名を削除する（S713）。これも、処理Aが、再帰的呼出しであるために、処理から抜けたときには、一番最後に追加されたドメイン名での探索は終了していることから必要になる処理である。

【0071】

この処理Aでは、再帰的な呼び出しを使っているために、クライアントからサーバへの道筋が複数ある場合にも、探索をすべての経路についておこなって、経由する可能性のある道筋をすべて見つけ出すことができることに注意しよう。

【0072】

ここで、図9を用いて「ドメイン1」に属するクライアントから「ドメイン3」に属するサーバにアクセスする場合に、設定するファイアウォールを特定する処理を具体的に説明しよう。まず、「ドメイン1」を経由ドメインリストの先頭に追加する（S71、図9（a））。次に、「ドメイン1」を処理Aに渡す引数として、経由ドメインリストを取得する処理A（S74）を開始する（S72）。まず、「ドメイン1」とドメイン名フィールド61が一致するエントリとして65aを検出し、その隣接ドメイン名フィールド63に記載された「ドメイン2」を隣接ドメインリストに加える（S75）。次に、隣接ドメインリストから「ドメイン2」を選択する（S76）。「ドメイン2」は経由ドメインリストにないので（S77）、「ドメイン2」を経由ドメインリストに追加する（S78、図9（b））。「ドメイン2」は、サーバドメイン名「ドメイン3」に等しくないので（S79）、「ドメイン2」を引数として、経由ドメインリストを取得する処理A（S74）を開始する（S712）。次に、「ドメイン2」を引数として、処理A（S74）を呼び出して、エントリ64bとエントリ64cから、隣接ドメインリストとして、「ドメイン2」と「ドメイン1」が得られる。「ドメイン1」の方は、既に経由ドメインリストに含まれているので、候補から省かれる（S77）。したがって、この段階で図9（c）に示される経由ドメインリストが得られる。

【0073】

次に、ドメイン名「インターネット」を引数として、処理A（S74）が呼び出される。

【0074】

「インターネット」をキーとして、得られる隣接ドメインは、エントリ64f, 64g, 64hから、それぞれ、「ドメイン2」、「ドメイン3」、「ドメイン4」である。

【0075】

「ドメイン2」は、やはり経由ドメインリストに既に存在しているので候補から省かれ、「ドメイン3」を経由ドメインリストに追加したときに、サーバドメイン名に等しくなるため（S79）、これを答えとして保存する（S710）。このあと、追加したドメインである「ドメイン3」を削除する（S711）。そして、図9（3）の状態に戻り探索を続けることになる。

【0076】

最終的に、図9（d）の状態のときの経由ドメインリストが、この処理の答えであって、「ドメイン1」、「ドメイン2」、「インターネット」、「ドメイン3」が取得できる。

【0077】

（2）ファイアウォール毎に設定情報を生成する処理192

次に、図11ないし図13を用いて管理サーバ13上のマネージャプログラム22が、各ファイアウォールに対して設定する情報を生成する処理について説明する。

図11は、管理サーバ13上のユーザ情報テーブル25を示す図である。

図12は、管理サーバ13上のファイアウォール設定情報テーブル215を示す図である。

図13は、登録IDを生成する処理を示すフローチャートである。

【0078】

（1）の処理により、設定対象のファイアウォールを特定した後、管理サーバ13上のマネージャプログラム22は、各ファイアウォールに対して設定する情報

を生成する。

【0079】

最終的に、必要な情報が生成されると、図11に示されるユーザ情報テーブル25と図12に示されるファイアウォール設定情報テーブル215に格納されることになる。ここで、ユーザ情報テーブル25は、ユーザ識別子（グローバルユーザ名）毎に、サービスを受けるときの利用形態と利用経路情報としてまとめたテーブルである。また、ファイアウォール設定情報テーブル215は、管理サーバのメモリ情報にダイナミックに作られるテーブルであり、後に説明するファイアウォールへ情報を設定するときのリクエストパケットを生成するとき用いられるテーブルである。

【0080】

（a）登録IDの生成

まず、マネージャプログラム28は、登録IDを生成する。登録IDとは、各ファイアウォールがサービスを受けるユーザに対して、認証をおこなうために用いる識別子である。これは、ユーザ毎、ファイアウォール毎に一意的な名称を用いる必要がある。

【0081】

これを図12に示したユーザ情報テーブル25のエントリ126cを例にとって説明しよう。

【0082】

（1）と（2）の処理が終わった段階で、グローバルユーザ名121「abc」、クライアントアドレス122「ドメイン1」、サーバアドレス123「ドメイン3」、サービス／プロトコル124「telnet/TCP」の値は設定されている。

【0083】

利用経路情報リストフィールド125には、[ファイアウォール名 登録ID]がペアとなって、リスト構造で格納される。このエントリ126cには、[ファイアウォール1 ABC]、[ファイアウォール2 ABc]、[ファイアウォール3 Abc]が格納されていることが示されている。これまで述べてきた

処理で設定対象となるファイアウォールは、ファイアウォール1、ファイアウォール2、ファイアウォール3であることは、求まっているので各々のファイアウォール毎に登録IDを生成する処理をおこなうわけである。

【0084】

次に、図13のフローチャートの順を追いながら、マネージャプログラム23が登録IDを生成する処理について説明する。

【0085】

マネージャプログラム23は、図11のユーザ情報テーブル25を検索することにより、入力画面51から取得したグローバルユーザ名52が、設定対象ファイアウォールに登録されているかをチェックする(S131)。登録IDは、グローバルユーザ名と、ファイアウォールが同じときには、同じになるものと約束するからである。

【0086】

ユーザ情報テーブルを検索して、登録されているときには(S132)、ステップ137に進む。

【0087】

登録されていないときには(S132)、登録ID候補を生成する(S133)。ここで、登録ID候補の生成処理は、第一候補をグローバルユーザ名をそのまま用いることにし、第二候補以降については、グローバルユーザ名の後ろに数字をつけたり(abc1, abc2, …)、大文字と小文字を変える(ABC, ABc, …)などの方法により実現できる。

【0088】

さて、登録IDは、各ファイアウォールで、サービスを受けるときに認証に使われるものである。したがって、同じファイアウォールで既にその登録ID候補が衝突することがないかを確認する必要がある。そのため、生成した登録ID候補を、ファイアウォール上のエージェントプログラム33に送信する(S134)。マネージャプログラムとエージェントプログラムとの間の登録ID候補の送受信は、Telnet等のアプリケーションと同様に、プロトコルとして、TCP/IPを用いることにして、両者の間でコネクションを確立し、そのコネクシ

ョン上でパケットを送受信することにより実現できる。

【0089】

ファイアウォール上のエージェントプログラム33は、送られてきた登録ID候補が、そのファイアウォール上で既に使われているか否かを確認し、その結果を管理サーバ上のマネージャプログラム22に送信する(S135)。その結果、その登録ID候補が設定対象ファイアウォール上で既に使われていることがわかれば(S136)、別の登録ID候補を生成する(S132)。

【0090】

まだ使用されていない場合には(S136)、それを登録IDとする。

【0091】

一つの設定対象の処理が終わると、次の設定対象ファイアウォールを取り出し、すべての設定対象ファイアウォールについて、同様にステップ131からステップ136の処理を繰り返す(S137)。

【0092】

そして、全ての設定対象ファイアウォールについて登録IDが確定したとき(S137)、ユーザ情報テーブル25にエントリを追加する(S138)。

【0093】

ここで、具体例を採って説明しよう。図11に示すユーザ情報テーブル121に、エントリ126aとエントリ126bだけが登録されているとし、図5に示す入力がおこなわれたとする。

【0094】

(1)の設定対象ファイアウォールを特定する処理により、設定をおこなうファイアウォールは、「ファイアウォール1」、「ファイアウォール2」、「ファイアウォール3」であることがわかっている。エントリ126aには、グローバルユーザ名が「abc」のユーザがファイアウォール1に登録ID「ABC」として登録されていることが分かるのでなにもしない(S131, S132)。

【0095】

ファイアウォール2とファイアウォール3については、該当する登録IDがないので、新規に登録IDを生成する。

【0096】

管理サーバ13上でファイアウォール2とファイアウォール3に登録する登録ID候補を、それぞれ「ABc」、「Abc」と生成したとする(S133)。

【0097】

マネージャプログラム32は、ファイアウォール上のエージェントプログラム33へそれらが使われていないと問い合わせおこない、それらが各々のファイアウォール上で使われていないという結果を得たとする(S134, S135, S136)。

【0098】

その結果により、登録IDとして、ファイアウォール2には「ABc」、ファイアウォール3には「Abc」を用いることが確定し、ユーザ情報テーブル25にはエントリ126cが図11の如く追加される。

【0099】

(b) ファイアウォール設定情報テーブル215の設定

これまで得られてきた情報を基にして、マネージャプログラム23は、最終的に、図12に示されるファイアウォール設定情報テーブル215に値を設定する。次の各設定対象ファイアウォールに対して設定情報を送信する処理の段階では、このテーブルを基にして、各設定対象ファイアウォールに対して送信する情報を生成するのである。

【0100】

ファイアウォール設定情報テーブル215は、図12に示される様に、設定対象ファイアウォール141、登録ID142、クライアントアドレス143、サーバアドレス144、サービス/プロトコル145、送信元アドレス146、送信先アドレス147から構成される。

【0101】

設定対象ファイアウォール141は、このテーブルのキーとなるフィールドであり、その名の如くその登録IDに関して設定対象となるファイアウォールのアドレスが格納される。

【0102】

登録ID142は、(a)で説明してきた登録IDが格納されるフィールドであり、クライアントアドレス143、サーバアドレス144、サービス/プロトコル145については、図11に示したユーザ情報テーブル25のときと同様である。

【0103】

送信元アドレス146は、このファイアウォールに対して、ユーザがサービスを受ける際に、パケットが直接送られてくる送信元のアドレスを示すフィールドである。逆に、送信先アドレス147には、ユーザがサービスを受ける際に、このファイアウォールが、パケットを直接送信する送信先のアドレスを示すフィールドである。これは、図11に示される様に、サーバやクライアントに直接接しているときには、サーバアドレスやクライアントアドレスがそのまま格納され、ファイアウォールを経由するときには、ファイアウォールのアドレスが格納される。

【0104】

この送信元アドレス146と送信先アドレス147は、ユーザ情報テーブル25のクライアントアドレス122、サーバアドレス123、および利用経路情報リスト125を基にして生成することができる。

【0105】

ここで具体例に基づいて説明しよう。

【0106】

図12のエントリ148bに示されている設定対象ファイアウォールが、「ファイアウォール2」であるときには、図11のユーザ情報設定テーブル25のエントリ126cに基づいて、登録ID142に「ABc」が、クライアントアドレス143に「ドメイン1」が、サーバアドレス144に「ドメイン3」が、サービス/プロトコル145に「telnet/TCP」が、それぞれ格納される。

【0107】

また、送信元アドレス146と送信先アドレス147には、利用経路情報リス

ト125の「ファイアウォール2」が格納されている前後のフィールドから、「ファイアウォール1」と「ファイアウォール3」が得られる。

【0108】

(3) ファイアウォール毎の設定情報を各ファイアウォールに送信する処理
193

次に、図14および図15を用いてマネージャプログラム23がファイアウォール毎の設定情報を各ファイアウォールに送信する処理193について説明する。

図14は、マネージャプログラム23が各ファイアウォールに送信するリクエストパケット151と、エージェントプログラム33が管理サーバ13に送信するリプライパケット1511のフォーマットを示す図である。

図15は、管理サーバ13上のマネージャプログラム23と、ファイアウォール上のエージェントプログラム33の通信プロトコルを示す図である。

【0109】

リクエストパケット151は、マネージャプログラム23が各設定対象となるファイアウォールに対して情報を設定するときに使われるパケットである。リクエストパケット151は、図14(a)に示される様に、コマンド152、作業対象153、登録ID154、クライアントアドレス155、サーバアドレス156、サービス/プロトコル157、送信元アドレス158、送信先アドレス159から構成される。このフォーマットは、必要なすべてのフィールドを挙げたものである。実際には、リクエストパケット151は、コマンド152、作業対象153毎に設定されるフィールドは異なっており、必要でないフィールドには、NULL値が設定されることになる。

【0110】

リプライパケット1511は、エージェントプログラム33がリクエストパケット151を受信したときに、ファイアウォール側で成否を示すために使われるパケットである。リクエストパケット151は、図14(b)に示される様に、リプライコード1512、コマンド1513、作業対象1514から構成される。

【0111】

さて、以下では図14に示した具体例に基づき説明しよう。

【0112】

ここで、設定対象と想定しているファイアウォールは、ファイアウォール2である。

【0113】

パケット1510aは、コマンド152が「ADD」、作業対象が「USER」とされるパケットである。これは、登録ID154のフィールドが「ABC」になっており、登録ID候補をファイアウォール2に登録するためのパケットである。

【0114】

パケット1510bは、コマンド152が「ADD」、作業対象が「ACCESS」とされるパケットである。このパケットが、リクエストパケット151の中で一番内容が多彩であり、送られてきた情報は、すべてファイアウォールのアクセス制御テーブル（後述）に格納される。各々のフィールドの意義はこれまで述べてきたとおりである。

【0115】

パケット1510cは、コマンド152が「ADD」、作業対象が「ROUTE」とされるパケットである。このパケットは、ユーザがサービスを受けるときのルーティング情報を設定するためのパケットである。サーバアドレス156のフィールドには、ユーザにサービスを提供するサーバのアドレス、送信元アドレス159には、サーバのアドレスに該当するパケットを受けたときに、中継先となるファイアウォールのアドレスが格納される。この例のパケットでは、ファイアウォール2が、「ドメイン3」にあるサーバのサービスを受けるパケットを受信したときには、中継先として、「ファイアウォール3」にパケットを送信することを指示するようになっている。送られてきた情報は、ファイアウォールの経路制御テーブル（後述）に格納される。

【0116】

マネージャプログラム23は、これらのパケットを設定対象であるファイアウ

オール2に送信する。

【0117】

ファイアウォール2のエージェントプログラム33では、設定が正常に終了したときには、リプライコード1512に「0」を設定して、リプライパケット1511を管理サーバ13のマネージャプログラム23に送り返す。設定が正常に終了できなかったときには、リプライコード1512に「1」を設定して、リプライパケット1511を管理サーバ13のマネージャプログラム23に送り返す。ここで、リクエストパケット151のパケット1510a, 1510b, 1510cに、それぞれ対応するリプライパケット1511が、パケット1515a, 1515b, 1515cである。

【0118】

マネージャプログラム23が、リプライコード1512が「1」のリプライパケット1511を受け取ったときには、再送信やエラー処理などのしかるべき処理をとることになる。

【0119】

次に、図15を用いて、管理サーバ13上のマネージャプログラム23と、ファイアウォール上のエージェントプログラム33が、リクエストパケット151とリプライパケット1511をやり取りするときの通信手順について説明しよう。

【0120】

マネージャプログラム23は、(1)で設定対象とされたファイアウォールにつき、そのファイアウォール上のエージェントプログラム33に対して、接続要求をおこなう(SQ161)。

【0121】

マネージャプログラム23とエージェントプログラム33の間で相互認証を行う(SQ162)。相互認証は、セキュリティを保つ上で必須の処理である。相互認証SQ162に成功すると、両者で暗号鍵を取得する処理をおこなう(SQ163)。暗号鍵が必要となるのは、両者がセキュリティを保持するために暗号通信をおこなうことを前提としているからである。

【0122】

一方、相互認証SQ162に失敗した場合には、そこで、そのファイアウォールに対する処理を打ち切り、他の設定対象ファイアウォール上のエージェントプログラムに対する通信処理に移る。

【0123】

暗号鍵取得処理SQ163が終わると、エージェントプログラム33が、通信が可能であることを通知する接続確認パケットをマネージャプログラム23に送信する(SQ164)。

【0124】

マネージャプログラム23は、接続確認パケットを受信して接続を確認した後で、エージェントプログラム33にリクエストパケット151を送信する(SQ165)。リクエストパケット151は、暗号化されて送られることに注意しよう。

【0125】

エージェントプログラム33は、暗号鍵を用いリクエストパケット151を復号して、その情報に基づき内部のテーブルに必要な値を設定する(SQ166)。そして、その成否をリプライパケット1511で、をマネージャプログラム23に通知する(SQ167)。

【0126】

マネージャプログラム23は、上記のシーケンスSQ161～シーケンスSQ167をすべての設定対象ファイアウォールに対して繰り返しおこなうことにより、複数のファイアウォールに対して、一括して必要な設定処理を実現することができる。

【0127】

なお、相互認証処理162は、ISO/IEC9798やX.509の認証方法に基づいて実装することにより、実現可能である。

【0128】

また、暗号鍵取得処理163については、例えば、マネージャプログラム23とエージェントプログラム33で生成したランダムデータを相互に交換し、両者

で共有した2つのランダムデータから同じ暗号鍵データを生成することにより、共有鍵方式の暗号通信をおこなうことが可能である。

【0129】

(4) 各ファイアウォールが設定情報を受信し、それを設定する処理194次に、図16ないし図18を用いて各ファイアウォールが設定情報を受信し、それを設定する処理194について説明する。

図16は、ファイアウォール2上のユーザ登録テーブル312を示す図である。

図17は、ファイアウォール2上のアクセス制御テーブル313を示す図である。

図18は、ファイアウォール2上の経路制御テーブル314を示す図である。

【0130】

図で示されている値は、すべてファイアウォール2を例に採ったものである。

【0131】

ユーザ登録テーブル312は、登録IDに対し、その登録IDに合致する通信サービスのパケットを通過させるか否かを判断するときの認証情報を保持するテーブルであり、登録ID91と、認証情報92から構成されている。この認証情報92は、ユーザに予め知らされていて、ユーザがサービスを受けるときに、そのクライアントから送信されてくる。ファイアウォールでは、その登録IDに合致する認証情報が等しい否かにより、ユーザの認証をおこなう。

【0132】

ファイアウォール2は、図14(a)に示された作業対象153が「USER」であるパケット1510aを受けたときに登録IDを設定し、それに対する認証情報を生成する。

【0133】

アクセス制御テーブル313は、ファイアウォール上の設定情報を持つテーブルとして、中心となるテーブルである。ファイアウォール2は、図14(a)に示された作業対象153が「ACCESS」であるパケット1510bを受けたときに、図17に示される如く、それぞれ対応するフィールドにエントリ107

aのように値を設定する。

【0134】

経路制御テーブル314は、ユーザがサービスを受けるときのパケットをルーティングするためのルーティングテーブルであり、送信先アドレス111と中継先アドレス112で構成されている。

【0135】

送信先アドレス111は、サービスを享受するためのサーバが属するドメインのアドレスである。また、中継先アドレス112は、送信先アドレス111に書かれたサーバのアドレスと一致するパケットが来たときに、それを中継するファイアウォールのアドレスである。

【0136】

この例では、ファイアウォール2が、ドメイン3に属するサーバにパケットを送るときには、中継先のファイアウォールは、ファイアウォール3になることを示している。すなわち、ファイアウォール2は、図14(a)に示された作業対象153が「ROUTE」であるパケット1510cを受けたときに、図18に示される如く、エントリ113のように値を設定する。

【0137】

(5) ファイアウォールが接続を中継する処理195

次に、図19および図20を用いてファイアウォールが他のファイアウォールに対する接続を中継する処理について説明する。

図19は、管理サーバ上とファイアウォール上の両者に置かれる中継経路テーブル171を示す図である。

図20は、管理サーバ13上のマネージャプログラム23と、ファイアウォール上の中継プログラム34、およびエージェントプログラム33の三者の通信プロトコルを示す図である。

【0138】

中継テーブル171は、他のファイアウォールに接続を中継するために用いられるテーブルである。これは、予め管理者がネットワーク形態を調べ、設定しておく必要がある。また、この中継経路テーブル171は、他のファイアウォール

に接続するために、ファイアウォールと管理サーバとの両者に置かれることに注意しておこう。

【0139】

この図の値は、管理サーバ13に置かれる中継経路テーブル171を想定している。すなわち、管理サーバ13上のマネージャプログラム23は、ファイアウォール3に設定するためのリクエストパケット151を送るときには、先ず、ファイアウォール2に対して接続要求をする。

【0140】

図には示さなかったが、ファイアウォール2上にある中継経路テーブル171には、送信先アドレス172が、「ファイアウォール3」で、中継先アドレス173も、「ファイアウォール3」のエントリがある。ファイアウォール2の中継プログラム34は、ファイアウォール3が設定対象のファイアウォールであったときには、自らの持つ中継テーブル171の中継先アドレス173を見て、ファイアウォール3に接続要求にいく。その後、相互認証と暗号鍵の取得などの処理をおこなった後に、管理サーバ13上のマネージャプログラム23は、リクエストパケット151を送信する。

【0141】

次に、この通信手順を図20を用いて説明しよう。

【0142】

マネージャプログラム23は、中継経路テーブル171のエントリ174aから、次の接続先をファイアウォール2(14b)に決定する(SQ181)。

【0143】

そして、ファイアウォール2(14b)の中継プログラム34に接続を要求する(SQ182)。

【0144】

接続要求後、マネージャプログラムと中継プログラムとが相互認証処理SQ183および暗号鍵取得処理SQ184をおこなう。

【0145】

相互認証および暗号鍵取得に成功した場合には、中継プログラム34は、ファ

ファイアウォール2（14b）上の中継経路テーブル171に基づいて、ファイアウォール3（14c）を中継先のファイアウォールであることを求める。その結果に基づいて、ファイアウォール2上の中継プログラム34は、ファイアウォール3に接続することを決定し（SQ185）、マネージャプログラム23にファイアウォール3（14c）に接続することを通知する（SQ186）。

【0146】

かつ、ファイアウォール2上の中継プログラム34は、ファイアウォール3（14c）上のエージェントプログラム33に接続要求をおこなう（SQ187）。そして、その後は、図15のシーケンスSQ161～シーケンスSQ167に従い、マネージャプログラム23とエージェントプログラム33との間で、相互認証処理SQ188、暗号鍵取得処理SQ189、接続確認SQ1810がおこなわれ、管理サーバ上のマネージャプログラム23と、ファイアウォール3上のエージェントプログラム33上で通信が開始されることになる（SQ1811）。

【0147】

すなわち、以上の手順により、マネージャプログラム23とエージェントプログラム33の間で、相互認証がおこなわれ、暗号で通信することが可能な安全なコネクションが確立することになる。

【0148】

なお、マネージャプログラム23と中継プログラム34との間の相互認証および暗号鍵取得の方法は、マネージャプログラム23とエージェントプログラム33との間の相互認証および暗号鍵取得の例と同じ方法が利用できる。

【0149】

〔ユーザがサービスを受けるときのファイアウォールの動作〕

次に、実際に、ユーザがクライアントからサーバに対して、サービスを受けるときにファイアウォールがどのように動作するかについて説明する。

【0150】

例として、図21および図23を用いて、図6に示した様にクライアントアドレスが「ドメイン1」で、サーバアドレスが「ドメイン3」で、サービス/プロ

トコルが「TCP/IP」であるときのファイアウォールの処理について説明しよう。

図21は、ファイアウォール1上のユーザ登録テーブル312を示す図である。

図22は、ファイアウォール1上のアクセス制御テーブル313を示す図である。

【0151】

図23は、ファイアウォール1上の経路制御テーブル314を示す図である。

【0152】

図1に示されたネットワークでは、ドメイン1(12a)からパケットが送信されるので、まず、ファイアウォール1(14a)のチェックを受けることになる。

【0153】

ファイアウォール1(14a)では、アクセスがあった場合に、図22に示されたアクセス制御テーブル313を検索し、どの登録IDに該当するを検索する。該当しない場合には、「サービスを受けるための登録ができていない」旨のメッセージを出し、ユーザのそれ以降のアクセスを拒否する。チェックに使う項目は、セキュリティの方針にしたがって、アクセス制御テーブルのすべての項目でチェックしても良いし、その一部の項目でチェックしても良い。

【0154】

この場合は、エントリ207aの登録ID101の「ABC」がこれに該当する。

【0155】

したがって、次に、図21に示されるユーザ登録テーブル312により、ユーザ認証をおこなう。クライアントの方から認証情報が送られてくるので、ファイアウォール1(14a)は、ユーザ登録テーブル312のエントリ293aの認証情報と、合致するか否かを確認する。

【0156】

認証情報は、アクセスするときに、ユーザがパスワードを入力するイメージで

ファイアウォール側にその認証情報を送信するか、システムが自動的にその認証情報を送信するようにすれば良い。

【0157】

認証情報が間違っているときには、「ユーザの認証が失敗した」旨のメッセージを出し、サービスは、拒絶されることになる。

【0158】

認証情報が正しく送られてきたことを確認されたときには、ファイアウォール1(14a)は、図23に示された経路制御テーブルを参照して、次のファイアウォール2(14b)にパケットを中継する。この場合のパケットの送信先アドレスは、ドメイン3なのでエントリ213aの中継先アドレスの値「ファイアウォール2」より次のファイアウォールが求められことになる。

【0159】

そして、パケットが中継されると、次のファイアウォール2(14b)でもおなじ処理がおこなわれる。

【0160】

ファイアウォール2(14b)では、図16に示されるユーザ登録テーブル312と、図17に示されるアクセス制御テーブル313とにより、アクセスの許可をする。用いられる登録IDは、「ABC」である。また、次の中継先を求めるのは、図18に示される経路制御テーブルであり、このエントリ113aにより、次の中継先がファイアウォール3であることを求める。

【0161】

このようにして、ファイアウォール1(14a)、ファイアウォール2(14b)、ファイアウォール3(14c)のすべてにアクセスが許可されたときに、初めて、ドメイン1にいるクライアントは、ドメイン3のサーバからtelnetのサービスを享受できる。不正なアクセス、認証を受けていないユーザは、接続を拒否され、システムに侵入することができない。すなわち、各ファイアウォールでは、かくして不正なアクセスからシステムを防御する防火壁の役割を果たすことができる。

【0162】

【発明の効果】

本発明によれば、イントラネット、VPNのような複数のファイアウォールを有するネットワークシステムにおいて、それらのファイアウォールを統括的に管理して、ファイアウォールに対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するファイアウォール統括管理システムを提供することができる。

【図面の簡単な説明】

【図1】

本実施形態に係るファイアウォール統括管理システムのネットワーク構成図である。

【図2】

本実施形態に係る管理サーバ13のハードウェア構成図である。

【図3】

本実施形態に係るファイアウォール14a～14dのハードウェア構成図である。

【図4】

本実施形態に係る管理端末15のハードウェア構成図である。

【図5】

本発明に係るファイアウォール統括管理システムが、ファイアウォールの設定をする処理を模式的に示した図である。

【図6】

管理者が、設定情報を入力するときの管理端末15上の入力画面51を示す図である。

【図7】

管理サーバ13上のファイアウォール構成情報テーブル24を示す図である。

【図8】

マネージャプログラム22が設定するファイアウォールを特定する処理を示すフローチャートである。

【図 9】

経路ドメインリスト 214 の内容を状態毎に示した図である。

【図 10】

管理サーバ 13 上の経路ファイアウォールテーブル 214 を示す図である。

【図 11】

管理サーバ 13 上のユーザ情報テーブル 25 を示す図である。

【図 12】

管理サーバ 13 上のファイアウォール設定情報テーブル 215 を示す図である。

【図 13】

登録 ID を生成する処理を示すフローチャートである。

【図 14】

マネージャプログラム 23 が各ファイアウォールに送信するリクエストパケット 151 と、エージェントプログラム 33 が管理サーバ 13 に送信するリプライパケット 1511 のフォーマットを示す図である。

【図 15】

管理サーバ 13 上のマネージャプログラム 23 と、ファイアウォール上のエージェントプログラム 33 の通信プロトコルを示す図である。

【図 16】

ファイアウォール 2 上のユーザ登録テーブル 312 を示す図である。

【図 17】

ファイアウォール 2 上のアクセス制御テーブル 313 を示す図である。

【図 18】

ファイアウォール 2 上の経路制御テーブル 314 を示す図である。

【図 19】

管理サーバ上とファイアウォール上の両者に置かれる中継経路テーブル 171 を示す図である。

【図 20】

管理サーバ 13 上のマネージャプログラム 23 と、ファイアウォール上の中継

プログラム34、およびエージェントプログラム33の三者の通信プロトコルを示す図である。

【図21】

ファイアウォール1上のユーザ登録テーブル312を示す図である。

【図22】

ファイアウォール1上のアクセス制御テーブル313を示す図である。

【図23】

ファイアウォール1上の経路制御テーブル314を示す図である。

【符号の説明】

11…インターネット、12a～12d…ドメイン、13…管理サーバ、14a～14d…ファイアウォール、15…管理端末、21…プロセッサ、22…固定ディスク、23…マネージャプログラム、24…ファイアウォール構成情報テーブル、25…ユーザ情報テーブル、26…中継経路テーブル、27…メモリ、28…マネージャプログラムエリア、29…認証・暗号通信モジュールエリア、210…中継経路テーブルエリア、211…入出力制御部、212…ディスプレイ・キーボード、213…ネットワーク制御部、214…経由ファイアウォールテーブルエリア、215…ファイアウォール設定情報テーブルエリア、31…プロセッサ、32…固定ディスク、33…エージェントプログラム、34…中継プログラム、35…中継経路テーブル、36…メモリ、37…エージェントプログラムエリア、38…中継プログラムエリア、39…中継経路テーブルエリア、310…認証・暗号通信モジュールエリア、311…ネットワーク制御部、312…ユーザ登録テーブル、313…アクセス制御テーブル、314…経路制御テーブル、41…プロセッサ、42…固定ディスク、43…ユーザインタフェースプログラム、44…メモリ、45…ユーザインタフェースプログラムエリア、46…入出力制御部、47…ディスプレイ・キーボード、48…ネットワーク制御部、51…入力画面、52…グローバルユーザ名、53…クライアントアドレス、54…サーバアドレス、55…サービス名、61…ドメイン名フィールド、62…ファイアウォール名フィールド、63…隣接ドメイン名フィールド、64a～64f…ドメインエントリ、71…リスト初期化处理、72…経由ドメイン検索

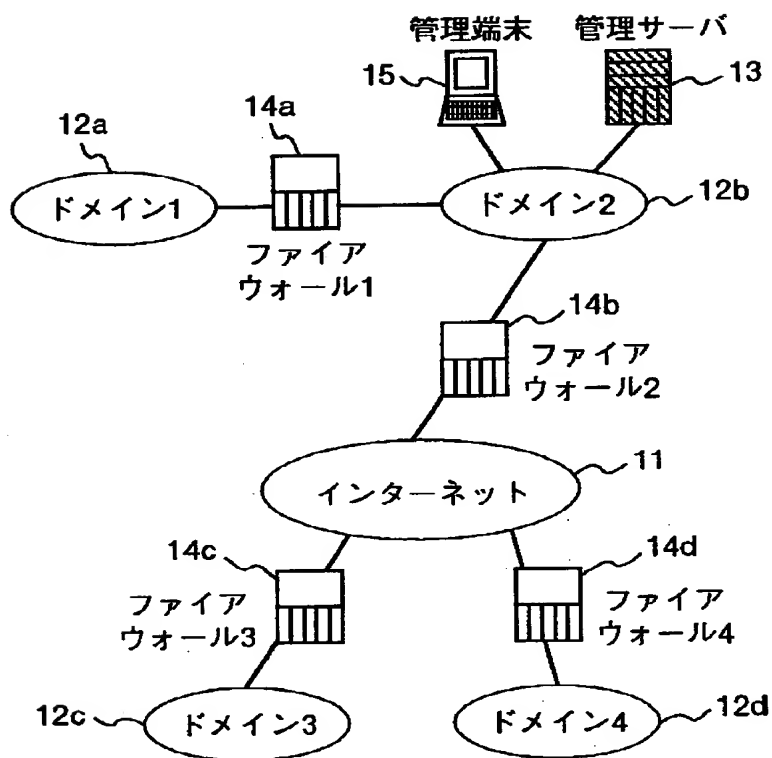
処理、73…経由ファイアウォール取得処理、74…隣接ドメイン名取得処理、75…リスト要素条件分岐処理、76…ドメイン名使用条件分岐処理、77…経由ドメインリスト追加処理、78…終了条件分岐処理、79…経由ドメインリスト保存処理、710…経由ドメインリスト削除処理、711…経由ドメイン検索再帰処理、712…経由ドメインリスト削除処理、81…クライアントアドレス、82…サーバアドレス、83…経由ファイアウォールリスト、91…登録IDフィールド、92…認証情報フィールド、93a, 93b…ユーザ情報エントリ、101…登録IDフィールド、102…クライアントアドレスフィールド、103…サーバアドレスフィールド、104…送信元アドレスフィールド、105…送信先アドレスフィールド、106…サービス名フィールド、107a, 107b…アクセス制御エントリ、111…送信先アドレスフィールド、112…中継先アドレスフィールド、113a, 113b…経路エントリフィールド、121…グローバルユーザ名フィールド、122…クライアントアドレスフィールド、123…サーバアドレスフィールド、124…サービス名フィールド、125…経由ファイアウォールリストフィールド、126a~126c…ユーザエントリ、131…ユーザ登録状況確認処理、132…ユーザ登録条件分岐処理、133…登録ID生成処理、134…登録ID送信処理、135…登録ID使用状況受信処理、136…登録ID使用条件分岐処理、137…登録確定条件分岐処理、138…テーブル登録処理、139…ファイアウォール設定情報生成処理、141…設定対象ファイアウォールフィールド、142…登録IDフィールド、143…クライアントアドレスフィールド、144…サーバアドレスフィールド、145…サービスフィールド、146…送信元アドレスフィールド、147…送信先アドレスフィールド、148a~148c…ファイアウォール設定情報エントリ、151…リクエストパケット、152…コマンドフィールド、153…作業対象フィールド、154…登録IDフィールド、155…クライアントアドレスフィールド、156…サーバアドレスフィールド、157…サービス名フィールド、158…送信元アドレスフィールド、159…送信先アドレスフィールド、1510a…ユーザ登録要求パケット、1510b…アクセス制御設定要求パケット、1510c…経路制御設定要求パケット、1511…リプライパケット

、1512…リプライコードフィールド、1513…コマンドフィールド、1514…作業対象フィールド、1515a…ユーザ登録処理結果通知パケット、1510b…アクセス制御設定処理結果通知パケット、1510c…経路制御設定処理結果通知パケット、161…接続要求処理、162…相互認証処理、163…暗号鍵取得処理、164…接続確認処理、165…リクエスト処理、166…設定実行処理、167…リプライ処理、171…経路制御情報テーブル、172…送信先アドレス、173…中継先アドレス、174a, 164b…経路エントリ、181…接続先決定処理、182…接続要求処理、183…相互認証処理、184…暗号鍵取得処理、185…接続先決定処理、186…接続確認処理、187…接続要求処理、188…相互認証処理、189…暗号鍵取得処理、1810…接続確認処理、1811…通信開始、191…設定対象ファイアウォール特定処理、192…ファイアウォール設定情報生成処理、193…設定情報送信処理、194…受信情報設定処理、195…接続中継処理、196…管理者、197…ユーザ、198…クライアント、199…サーバ。

【書類名】 図面

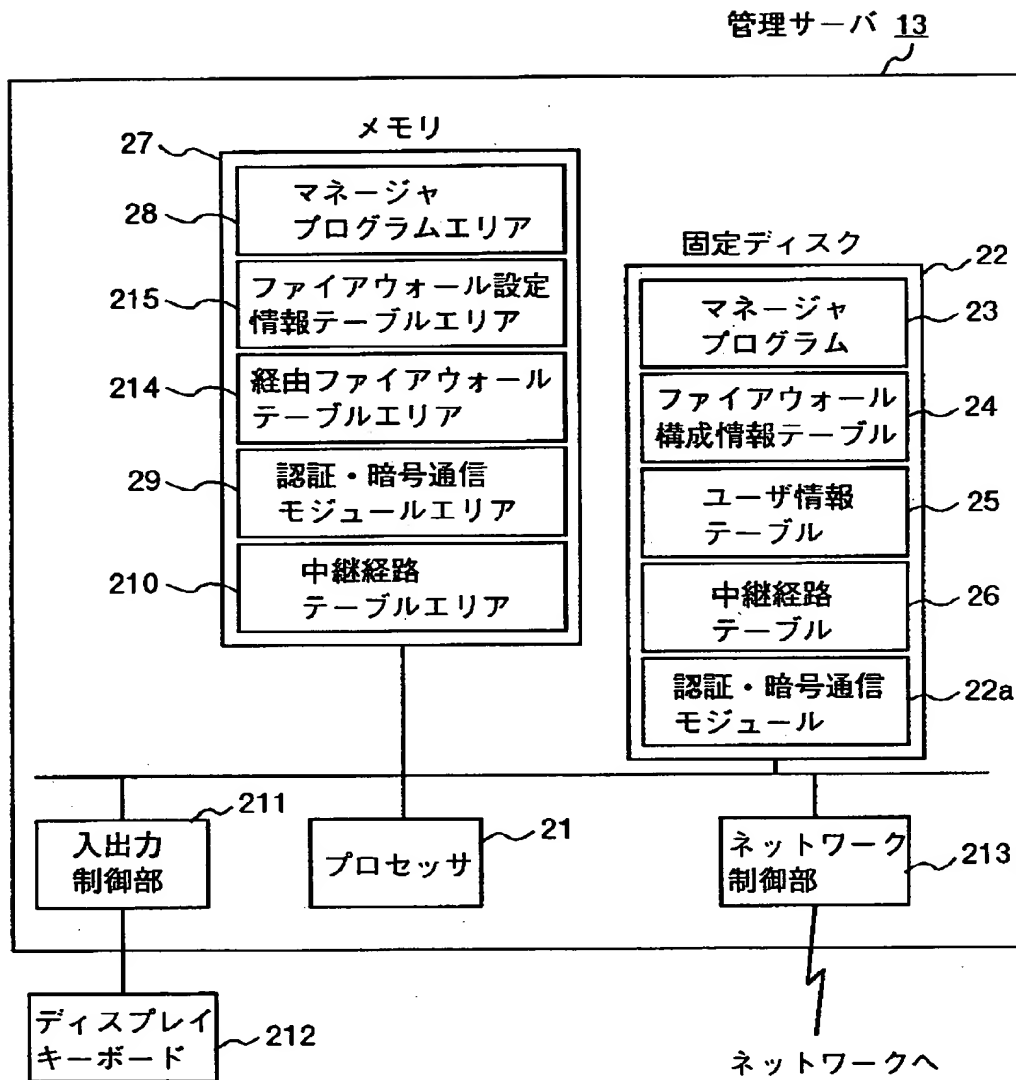
【図1】

図 1



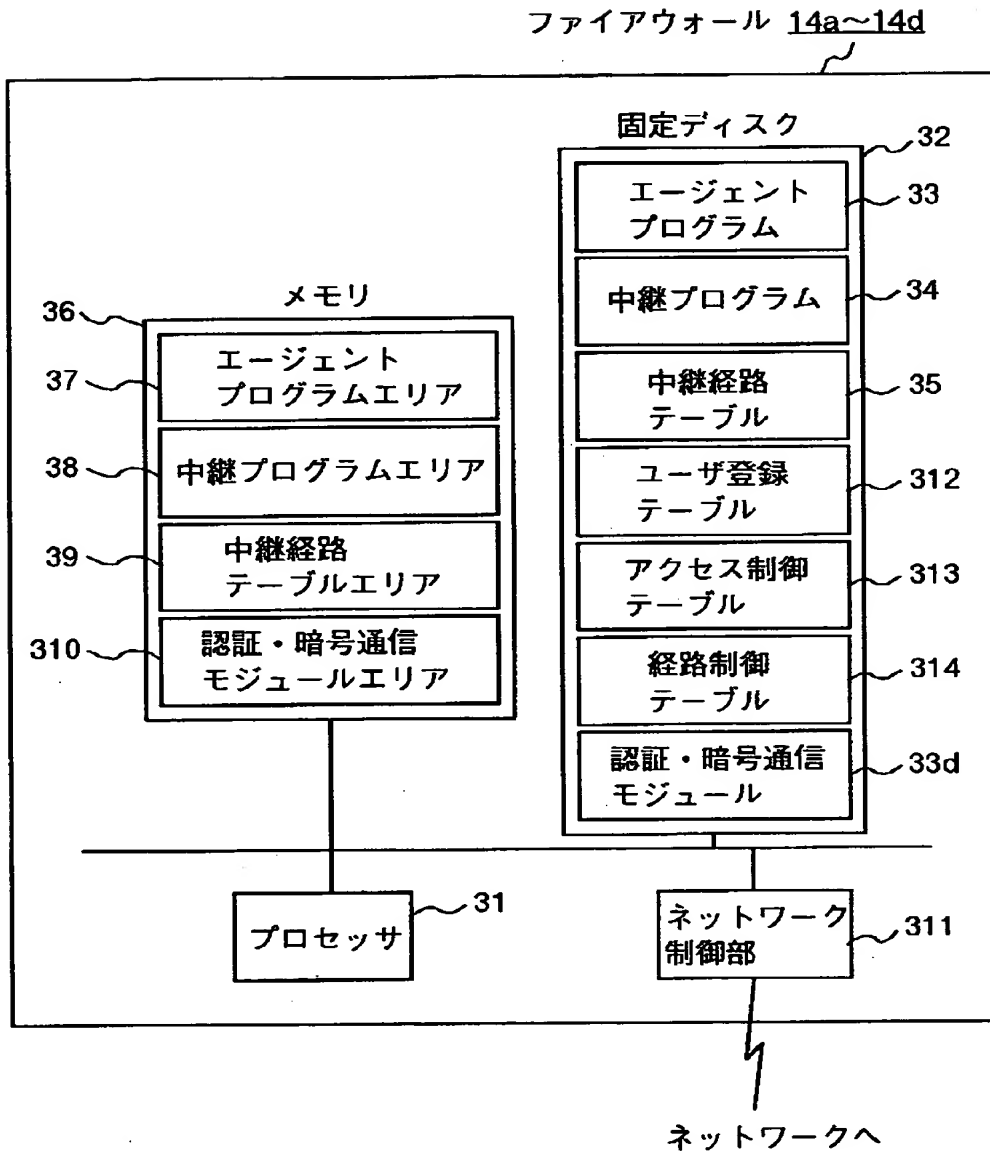
【図 2】

図 2



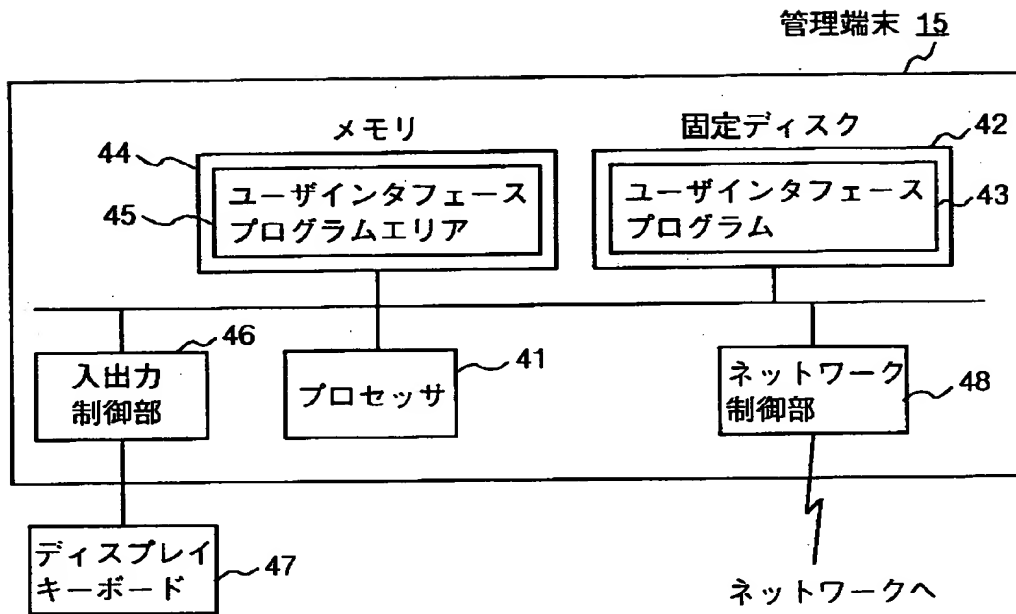
【図 3】

図 3



【図 4】

図 4



【図5】

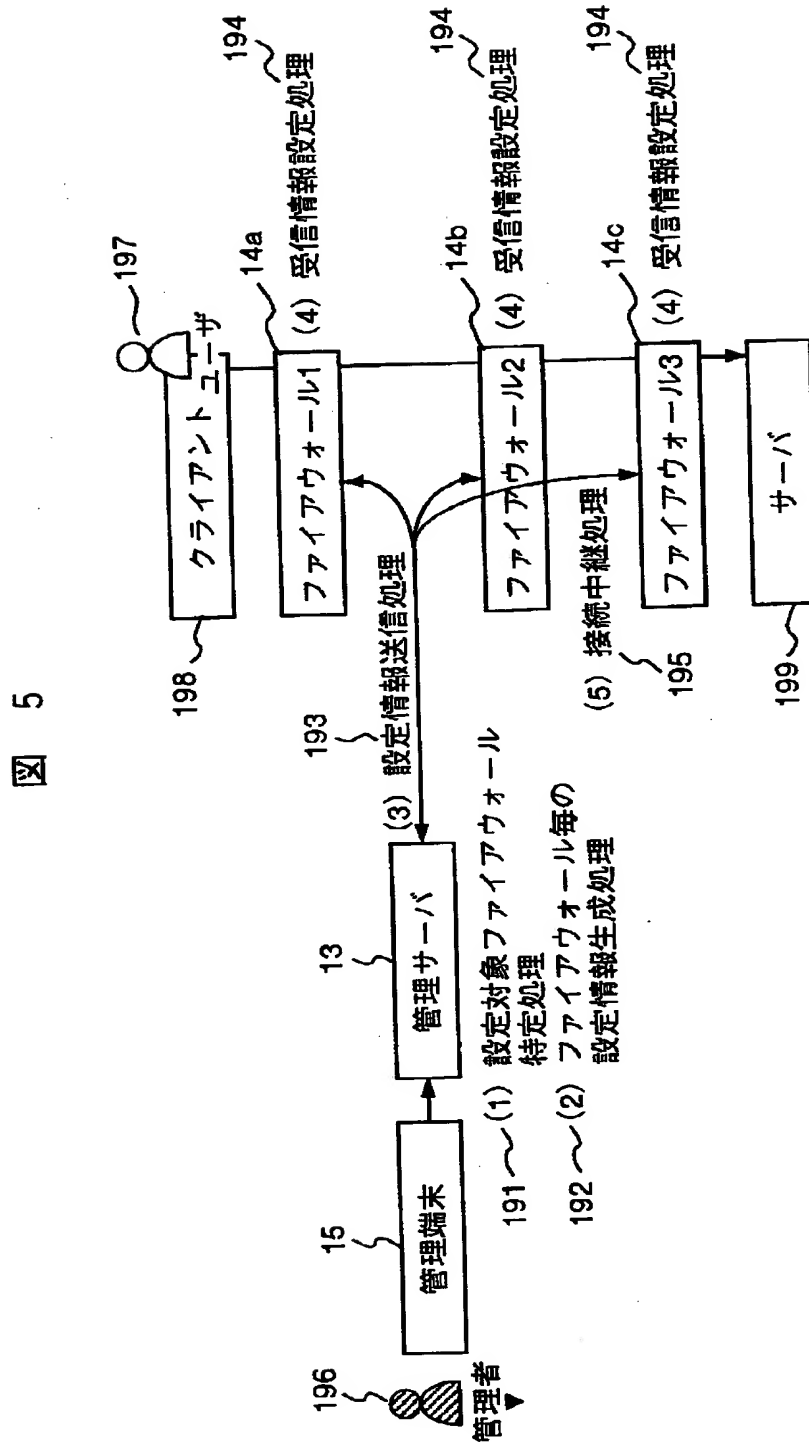


図5

【図 6】

図 6

グローバルユーザ名: abc

クライアントアドレス: ドメイン1

サーバアドレス: ドメイン3

サービス/プロトコル: telnet/TCP

OK CANCEL

【図 7】

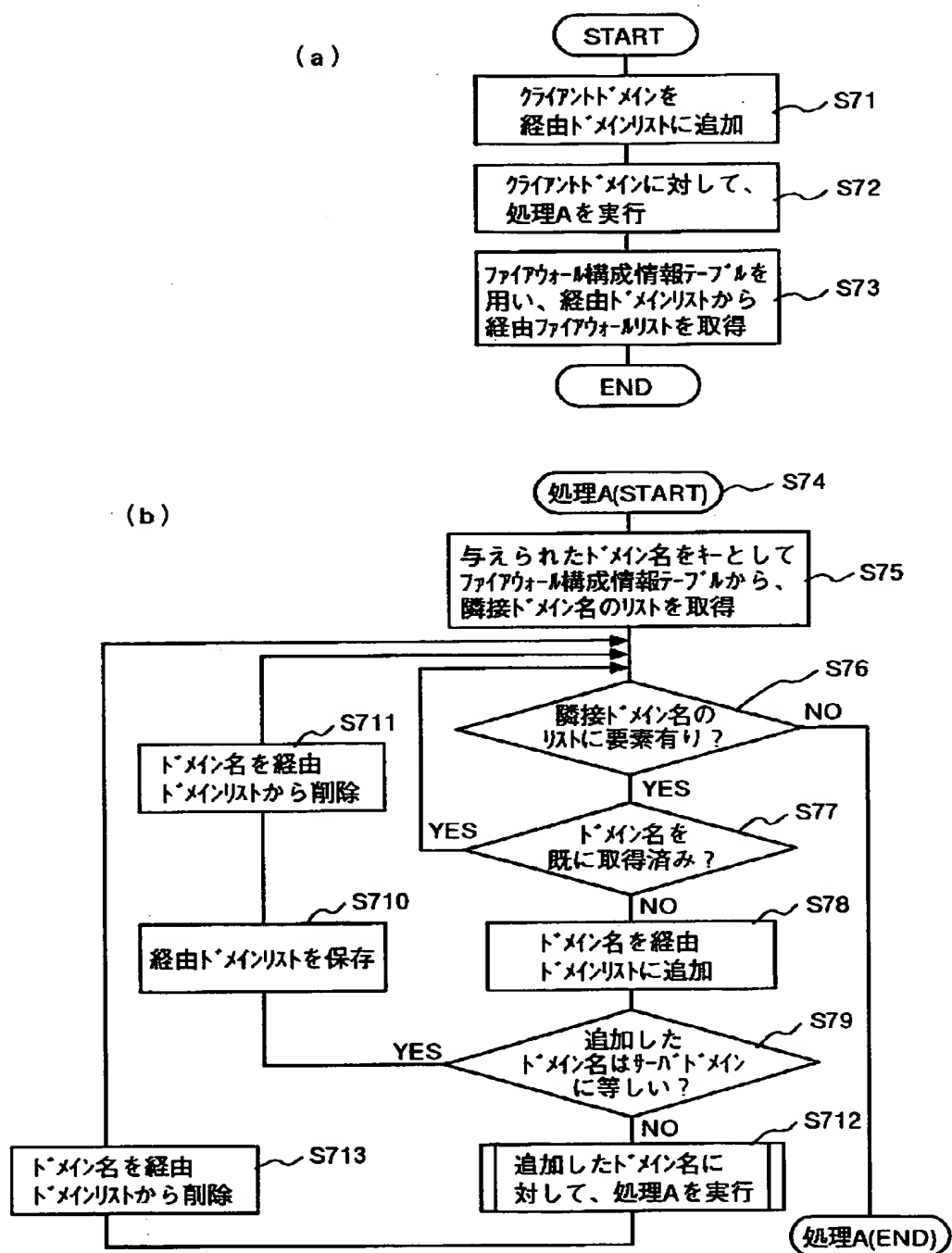
図 7

ファイアウォール構成情報テーブル 24

	61 ドメイン名	62 ファイアウォール名	63 隣接ドメイン名
64a	ドメイン1	ファイアウォール1	ドメイン2
64b	ドメイン2	ファイアウォール2	インターネット
64c	ドメイン2	ファイアウォール1	ドメイン1
64d	ドメイン3	ファイアウォール3	インターネット
64e	ドメイン4	ファイアウォール4	インターネット
64f	インターネット	ファイアウォール2	ドメイン2
64g	インターネット	ファイアウォール3	ドメイン3
64h	インターネット	ファイアウォール4	ドメイン4

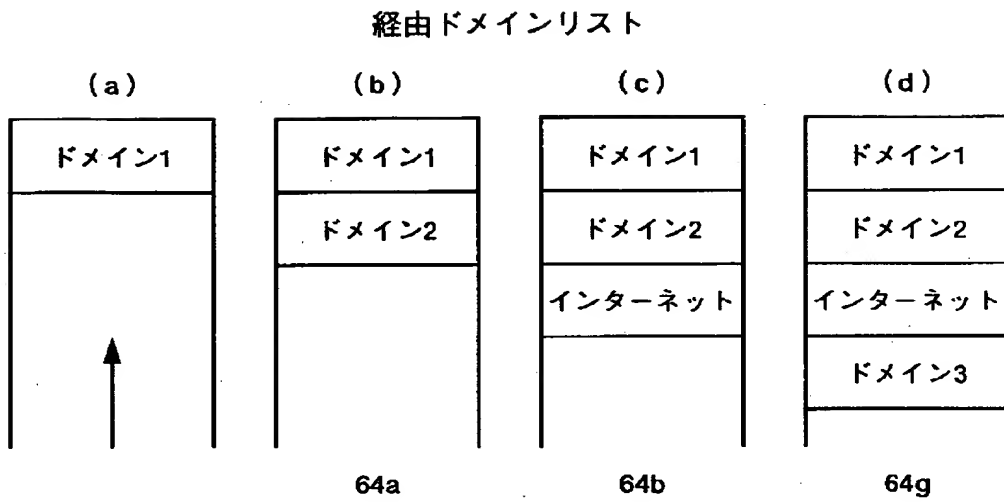
【図8】

図 8



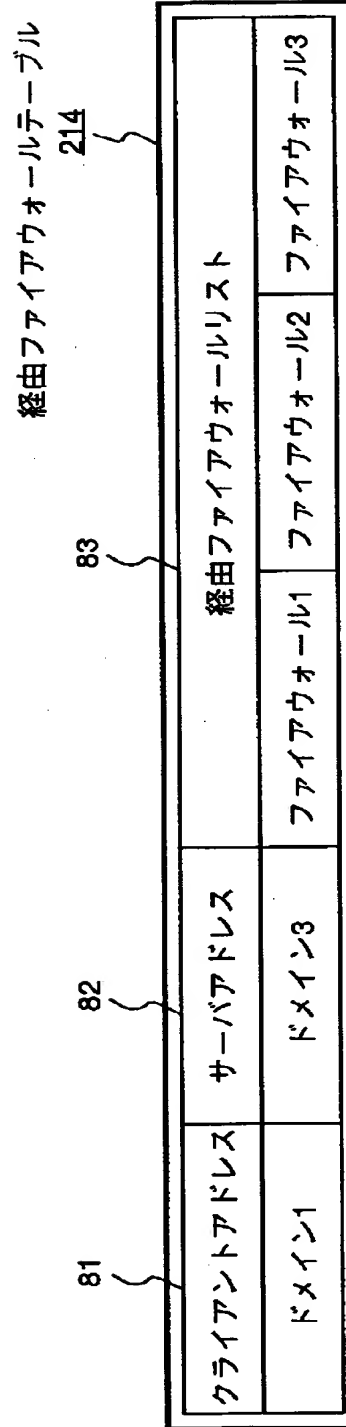
【図 9】

図 9



【図 10】

図 10



【図 11】

図 11

利用形態情報				利用経路情報		
121 統括 ユーザ名	122 クライアント アドレス	123 サーバ アドレス	124 サービス/ プロトコル	125 ファイアウォール名 登録ID	リスト	
abc	ドメイン1	ドメイン2	ftp/TCP	ファイアウォール1 ABC		
	ドメイン3	ドメイン4	ftp/TCP	ファイアウォール3 cde		
def				ファイアウォール4 CDE		
abc	ドメイン1	ドメイン3	telnet/TCP	ファイアウォール1 ABC	ファイアウォール2 Abc	ファイアウォール3 Abc

ユーザ情報テーブル 25

【図 12】

図 12

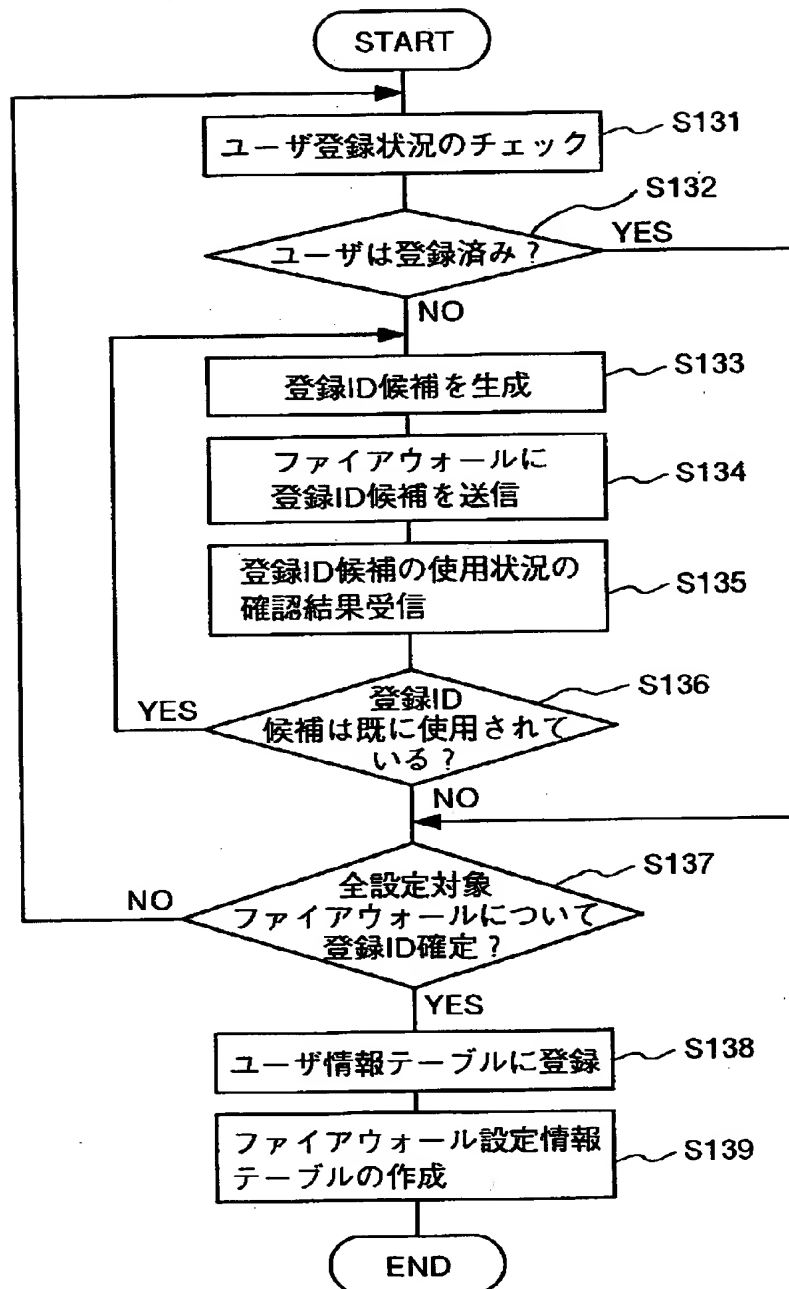
ファイアウォール設定情報テーブル

141	142	143	144	145	146	147
設定対象 ファイアウォール	登録ID	クライアント アドレス	サーバ アドレス	サービス/ プロトコル	送信元アドレス	送信先アドレス
ファイアウォール1	ABC	ドメイン1	ドメイン3	telnet/ TCP	ドメイン1	ファイアウォール2 148a
ファイアウォール2	ABc	ドメイン1	ドメイン3	telnet/ TCP	ファイアウォール1	ファイアウォール3 148b
ファイアウォール3	Abc	ドメイン1	ドメイン3	telnet/ TCP	ファイアウォール3	ドメイン3 148c

215

【図 13】

図 13



【図 14】

図 14

(a)

152	153	154	155	156	157	158	159	161
コマンド	作業対象	登録ID	クライアント アドレス	サーバ アドレス	サービス/ プロトコル	送信元 アドレス	送信先 アドレス	
ADD	USER	ABc	NULL	NULL	NULL	NULL	NULL	1510a
ADD	ACCESS	ABc	ドメイン1	ドメイン3	telnet/ TCP	ファイア ウォール1	ファイア ウォール3	1510b
ADD	ROUTE	NULL	NULL	ドメイン3	NULL	NULL	ファイア ウォール3	1510c

リクエストパケット

(b)

1512	1513	1514
リブライ コード	コマンド	作業対象
0	ADD	USER
0	ADD	ACCESS
0	ADD	ROUTE

1511 リブライパケット

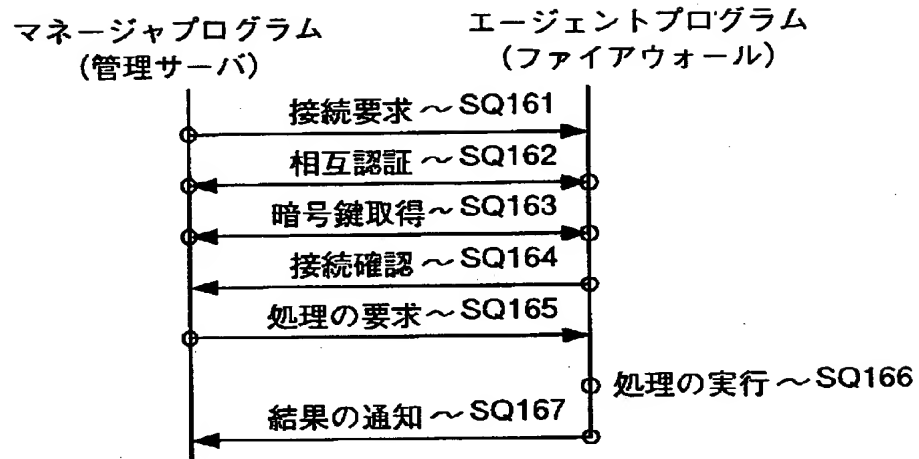
1515a

1515b

1515c

【図 15】

図 15



【図 16】

図 16

ユーザ登録テーブル

91	92	312
登録ID	認証情報	
ABc	x81.i!ht-v	93a
def	j" k2n# am+	93
⋮	⋮	

【図17】

図 17

アクセス制御テーブル 313

101	102	103	104	105	106
登録ID	クライアント アドレス	サーバ アドレス	送信元アドレス	送信先アドレス	サービス/ プロトコル
ABc	ドメイン1	ドメイン3	ファイアウォール1	ファイアウォール3	telnet/ TCP
def	ドメイン4	ドメイン2	ファイアウォール3	ドメイン2	ftp/ TCP
⋮	⋮	⋮	⋮	⋮	⋮

107a

107b

【図 18】

図 18

経路制御テーブル 314

送信先アドレス	中継先アドレス
ドメイン3	ファイアウォール3
ドメイン4	ファイアウォール4
⋮	⋮

111 112 113a 113b

【図 19】

図 19

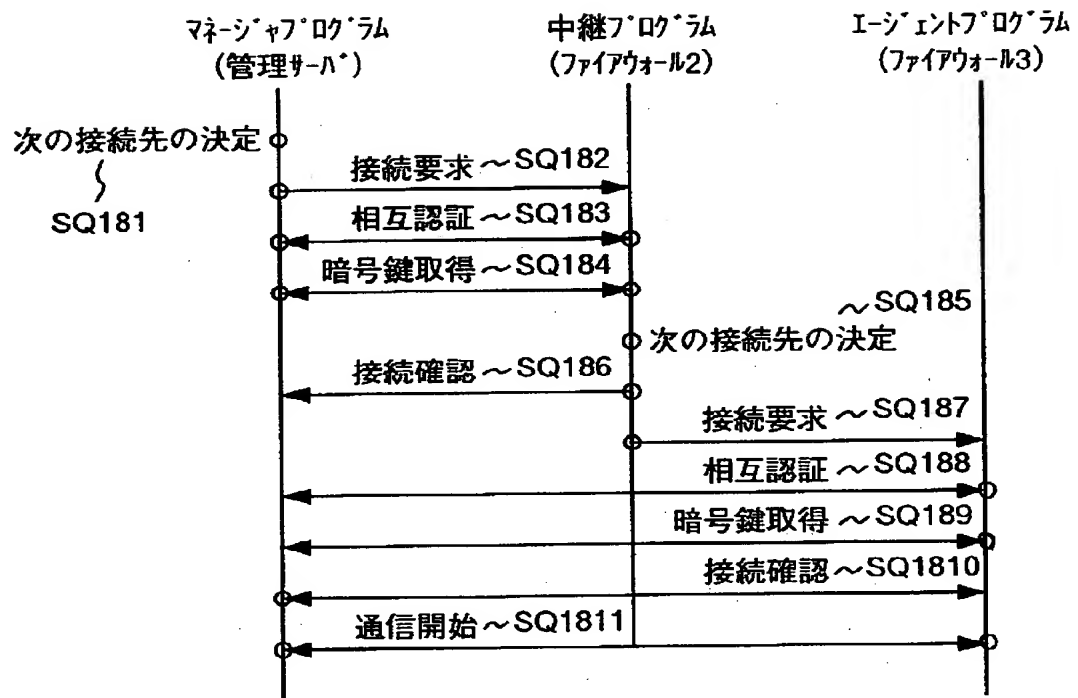
中継経路テーブル 171

送信先アドレス	中継先アドレス
ファイアウォール3	ファイアウォール2
ファイアウォール4	ファイアウォール2
⋮	⋮

172 173 174a 174b

【図 20】

図 20



【図 21】

図 21

ユーザ登録テーブル

登録ID	認証情報
ABC	a1314# #S
XYZ	fg2564++
⋮	⋮

Labels in the diagram:

- 91: Points to the registration ID column.
- 92: Points to the authentication information column.
- 312: Points to the entire table.
- 293a: Points to the first row of data.
- 293b: Points to the second row of data.

【図 22】

図 22

アクセス制御テーブル 313

登録ID	クライアント アドレス	サーバ アドレス	送信元アドレス	送信先アドレス	サービス/ プロトコル
ABC	ドメイン1	ドメイン3	ファイアウォール1	ファイアウォール3	telnet/ TCP
⋮	⋮	⋮	⋮	⋮	⋮

207a 207b

【図 23】

図 23

経路制御テーブル
314

111	112
送信先アドレス	中継先アドレス
ドメイン3	ファイアウォール2
⋮	⋮

213a

【書類名】 要約書

【要約】

【課題】 イントラネット、VPNのような複数のファイアウォールを有するネットワークシステムにおいて、ファイアウォールに対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するようにする。

【解決手段】 ネットワークの管理単位間にファイアウォールを設け、ファイアウォールに管理情報の設定をおこなうための管理サーバを置いて、その管理サーバのマネージャプログラムから、設定情報を送信することによって、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなう。また、途中のファイアウォールは、接続の中継をする。

【選択図】 図5

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000005108
【住所又は居所】 東京都千代田区神田駿河台四丁目6番地
【氏名又は名称】 株式会社日立製作所
【代理人】 申請人
【識別番号】 100061893
【住所又は居所】 東京都中央区日本橋茅場町二丁目九番八号 友泉茅
場町ビル 日東国際特許事務所
【氏名又は名称】 高橋 明夫
【選任した代理人】
【識別番号】 100086656
【住所又は居所】 東京都中央区日本橋茅場町二丁目九番八号 友泉茅
場町ビル 日東国際特許事務所
【氏名又は名称】 田中 恭助

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所